**DCJ 720 Written 4: Semi-Structured Interview**

Robert Chapa

Saint Leo University

Date of interview: 4/14/2022 2:15 PM

Location: Pasco Hernando State College student lounge

Topic: Organizational perceptions of cybersecurity

Respondent: White male cybersecurity expert with 15 years in the industry employed at local college.

|  |  |
| --- | --- |
| 2:15 PM  Interviewer:  Respondent:  Interviewer:  Respondent:  Interviewer:  2:22 PM  Respondent:  Interviewer:  Respondent:  Interviewer:  2:29 PM  Respondent:  Interviewer:  Respondent:  Interviewer:  Respondent:  Interviewer:  2:38 PM  Respondent:  Interviewer:  Respondent:  Interviewer:  Respondent:  Interviewer:  2:43 PM  Respondent:  Interviewer:  Respondent:  Interviewer:  Respondent:  Interviewer:  2:45 PM  Respondent:  Interviewer:  Respondent:  Interviewer:  Respondent:  Interviewer: | It is nice to meet you. As I said on the phone this should not take more than 20 or 30 minutes. I really appreciate you taking the time today to meet with me and allow me to interview you on cybersecurity. I was hoping that we would get along great because I also have a cybersecurity degree although I admit I ended up teaching and finally running MIS but we have similar backgrounds (chuckle).  No problem, I knew you had a cybersecurity degree because I heard other people talking about it. Do you have any certifications?  No, my interests were always academic, and I just never had enough time to pick up some certifications together with the degree. Speaking of certifications which ones do you have?  I have the certified ethical hacker and the compTia Security+ certification. What I really want though is the CISSP. That is the certified information systems security professional. If I can get that one. If I can just make the time to get that one I can get a job anywhere making well over six figures.  Those would be really nice to have. My first interview question is why did you choose the occupation of cybersecurity professional?  Eh, well, I grew up in the 90s and really enjoyed watching movies about hackers. Think it was about 1996 or so the movie “Antitrust” came out. I do not know if you saw that one or not but it was about a hacker who was recruited to company and he ends up finding out that the company is extremely corrupt even involved in murder to advance its technological goals. The main character a guy by the name of Milo also finds out that even his girlfriend from college was planted by the corporate company to entice him to work for them. There was a really good movie. Anyways, I started thinking about programming as a career. I know it seems kind of weird getting the programming because of the movie about coding[chuckle]. These days almost everyone I work with got into programming because they wanted to write code for computer games I feel like the computer world has been saturated with gamers or wannabe gamers. It is kind of funny if you think about it because there really are not that many jobs for gamers and so these kids are out of school picked up a couple languages and cannot get a job and then end up working for some IT department. It’s really sad.  That was really fascinating so did you have other influences that pushed you into the field of cybersecurity such as family members?  My parents did not understand what cybersecurity was and remember it was not really a term back then. The only thing they understood was that I wanted to get into computers. Of course, in the 90s computers had just gone mainstream with Microsoft putting out the Intel chip and homes getting Internet connections. You might remember the old ISPs that used your phone connection and get a baud rate of 14.4 or something. If you had told me back then that I would be sitting at home playing video games on an Internet connection of over a gig I would have said you were crazy. I still cannot believe the advances in technology that we have in our homes today (silence).  Can you tell me a little bit more about the role your family played those specifically her parents?  Oh yeah, sorry I have a lot on my mind I was getting to that. I do not really remember my dad saying too much about it he was just glad I was going to college since he had not gone. My mom on the other hand she was really excited about me getting into the computers and kept telling me I was making a great decision in the mid-1990s computers were still exotic to most people. So yes are going to college and be encouraged to study computer science was definitely encouraged by mostly my mom. But remember nobody was using the word cybersecurity back then,  That was really interesting could you please walk me through a cybersecurity incident that you have had recently?  Hum, well, I am happy to say that we have not had any major cybersecurity incidents in the last few years. That is not to say we are constantly hardening our systems to defend against an attack. So, the incidents that do happen are isolated to a small group of people or usually just one person. A Couple of months ago we had a student claim that her student account had been hijacked. I checked all the usual security applications looking for a breach but I did not see any alerts or any red flags. Did notice that the IP address that had looked at her account did not match the IP addresses that she had been using. It turned out that another student had guessed her password and accessed her online account. This kind of thing happens from time to time, and it is almost always the end-user’s fault because they do not follow good password protection protocols. We only recently started to offer two-factor authentication which adds that extra step for accessing accounts. But it is difficult to please everyone because now there is just one more thing that an end-user has to do, and they forget their security questions/answers. Thankfully, though we have not had any major breaches, especially toward databases or networks. That is mostly due to the fact that we keep those locked down really tightly.  How did you react to the incident?  Whenever this security call comes in, I do feel my heart rate increase [laughing]. My biggest fear of course is a full breach of our databases. Especially with the ransomware attacks that happen all the time these days. And even though we do everything we can to prepare ourselves for this type of breach it is never enough, and they could still happen. So the usual step is to check the software and look for an indications of a breach. After that, I look at the IP addresses see if anything unusual happened. Later, I need to talk to the student or the person who reported the incident. Try and find out everything I can about what happened why they think it happened you know the usual stuff. In her case she been locked out of her account so she could not change anything on her own. But once I validated that she was who she says she was then I opened up her account and changed her credentials and helped her set up two factor authentication. I also explained to her the necessity for a more complex password. In her case she volunteered that she had used the same password for her other accounts so that we would be easy to remember. Of course, you know that the major major no-no. She was really lucky that the person that had locked her out of her account had not thought to try to access her social media accounts or she would have had a real nightmare on her hands.  How did you work with administrators to address the incident?  The administration takes things very seriously. When a student complained to their advisor which is usually who they go to I will eventually get a call asking to help the student make sure that the security violation was not too extreme or especially that it does not impact the college. Once I began my investigation, I give an email report to my boss and explain the situation and what I am going to do to handle it. After collecting all information going through all the different security alerts and logs and handling the interviews with everyone involved then there is a form, I have to fill out that details the entire security event. That form then gets submitted to the VP of IT will submit it to the senior leadership. If there are any questions or issues log in an email asking to expand on whatever questions I have. Really, the administration is only concerned with major breaches. If the organization or college has a breach that makes the news or gets an email from someone in the senior leadership wanting reassurances about our security and what I am doing to handle any similar situations. Sometimes it can be a little annoying, but it is good to know that the administration here takes things seriously.  Discuss what your biggest fears are when reviewing security alerts.  : well, as I said already the biggest fear is breaches of the databases. Especially the financial or student databases. A major breach like that could end up shutting down the college for weeks maybe even months. Personally, I think it would be impossible for the college to recover from a breach like that. Not to mention the fact that I would lose my job. So, I guess you could say some type of ransomware attack that locks down the systems or exposes all of our data online. I am kind of thankful that I work at a college and not a major critical infrastructure like oil or gas or something. With all the stuff going on in Ukraine and the number of Russian attackers that hit our country their primary targets are going to be electricity some type of critical infrastructure not so much for colleges. So even though that would be a major hit it does give me some comfort to know that a college is probably not a primary target of state-sponsored terrorism or something like that.  Talk about the impact of the security monitoring software on the amount of time you spend checking articular notices.  All the security morning software sends out alerts or messages to my cell phone. So, I do not really have to check anything unless I receive a notice that there has been some suspicious activity, I will say that I feel a little bit of anxiety when an alert goes off on my phone. I have my phone set up with a certain tone for a security issue. It does not go off very often when it does, I get a little bit scared, but it is usually something minor that can be looked at and plugged so that sometimes goes off because the patch did install correctly or I need to double-check the vulnerability of the network port something like that. As far as logging in and making sure everything is good to go that is usually my first step in I get into the office in the morning my first check it from home on my laptop but then I realized it was just causing more anxiety so long as all get some type of serious security alert I will check anything until I get to the office and light up my systems. Now, I’ll go through all the different applications and double-check to make sure everything is good to go about it.  Please discuss the level of confidence you have in your organization’s security monitoring software.  Well I feel pretty confident about it we have several layers of security monitoring software that checks the ports suffer the checks the update of our servers and systems software the checks all the network settings software the checks all known vulnerabilities when we do everything we can to provide good cybersecurity for the college and I am confident that it will catch anything known but as you know from your own education we cannot provide hundred percent security if someone with sufficient skill is determined to initiate an attack on the college will work. All we can do is the best we can to make sure that the damage is limited. I do feel however that moving all the major sensitive databases to a cloud solution was the right decision the cloud providers that were using have a solid reputation for security and can provide additional layers that we simply cannot do here locally our own servers. So here it is a bit scary but I feel that we have done all we can and I have confidence in our systems and processes.  How does your administration demonstrate its commitment to cybersecurity?  IT equipment is pretty good. Like I said already we have a pretty solid budget, and we have an administrative board that takes cybersecurity very seriously like it like I said I can always tell because of the nature of the questions and the fact that I get a lot of emails or phone calls warning assurances that everything is okay. I mean at my last job before I came here I had the company was very profit-focused and so they would always cheap out when it came to security budgets and that felt like the administration just wanted to play the ostrich and put their head in the sand. This is terrible logic.  You mentioned that the college administration will email you and want assurances. Could you expand on their concerns a little bit.  Well like I said any time cybersecurity until it hits the news in order to call me and ask if we are covered I cannot remember what college it was a few months ago that all student data was vulnerable and that they had to shut down for a while. After that one there was a time when everybody started calling me in wonder where we stood so their concerns are legitimate and you have to remember none of these people are techs they’re just hoping and praying that I and my team are doing everything we can to keep things safe and so I feel that their commitment is pretty solid and that their concerns are our legitimate. I do like knowing that if I voice an opinion about the budget item that on more than likely going to get it so I have to say the commission administration is good or well-funded in the cybersecurity part of the head of IT.  Please explain the IT plan for dealing with a ransomware attack?  For working at public organization vs. the private sector. In this organization were not so worried about the loss of profits or billions of dollars. We can concentrate more on what the impact means for the loss of students and the reputation hit to the college. So, the plan that there is a report called an incident response report or critical incident response I think that is the name of it that I encountered. So that report must be filled out and there is a list of a checklist of items that must be reviewed before we can move forward with anything and so I go through the list and remember I have not had to do this for real thank goodness. We have not had a ransomware attack or a breach. But if we had one I would go through the checklist and part of that checklist the court is informing the senior leadership and my boss the VP of IT eventually we would have to report it to the state and federal authorities the report titled federal authorities would probably be within 24 hours would we have a small window to double-check everything make sure the breach is legitimate to make sure that we have our ducks in a row as to what we think may have happened did not and to try and handle the breach but regardless though that reports can go up the chain. So again, I have not had to go through the process in the real world but there is a checklist with a whole bunch of items that the help that I would have to go through I do not have it memorized. It,.. there is a whole bunch of things some of them are technical such as shutting down servers and locking things down. I,. we have consultants we would call in reporting part for the administration that it is a lengthy document, and I did not bring it with me. I did know I would be talking to this level but that it is a lengthy serious series of steps.  Please explain what conditions the administration would pay hackers to remove the ransomware?  That is an easy one under no conditions would the college pay malicious actors to remove ransomware. You see that kind of thing in the private sector because every minute of downtime is a loss of revenue and profit. At a state organization or public institution like we are that would not even be on the table. I can tell you there is no one within the administration of this college that would support a decision like that.  How has the administration adjusted the physical security of sensitive computing devices such as data centers, routers, etc.?  I spoke a little bit about this earlier. The single most critical change is the move to a cloud-based system. Retiring our servers is plugging a huge vulnerability hole. Like I said already the security of the cloud is stronger than what we can provide locally because they have a much higher budget and employ cybersecurity professionals were much stronger because of what they are paid for the job. If you look at the cloud solutions that have been hacked all of them have been non-education related. A few years back Sony’s cloud solution was hacked by Korean hackers. They had been provoked by a movie that Sony put out marking their leader. Again because of the nature of colleges as educational institutions we are a less likely target. I am not saying it could not happen and probably will happen at some point or who knows but I am saying that the security that the cloud services offers is stronger and more robust than what we can offer locally are also less points of failure. So the physical security side of the organization becomes less serious. If there is a vulnerability that I can think of it is probably that the user could have been jacked directly into the network via an ethernet cable or something. Connections are monitored. Classrooms do not have cameras in them. So, someone with sufficient skill could walk in and jack into a cable and initiate a hack. Because we are an educational institution with all sorts of people walking through our doors are open to our computer labs. It is impossible to provide physical security without locking out the students.  Okay, that has been a little over 30 minutes now. That was a fascinating look into the life of a Cybersecurity expert that you gave there. I just want to say thank you for your time. I learned a lot today. And keep up the good work! |

**Memo**

Thomas works in cybersecurity as a cyber expert, I was delighted to interview him. We met in a quiet lounge on campus because there are not many students on campus right now. The environment was also secluded and provided an excellent venue for an interview.

Thomas showed up on time. We had short introductions and began the interview. His mood was exciting and helpful. Although Thomas only had a bachelor's degree, he held a few industry cybersecurity certifications, making him extraordinarily strong and knowledgeable. He expressed sincere interest in meeting with me since I also had a strong background in cybersecurity minus the certifications. It was easy for Thomas to open up to me about his work because he knew that I would understand his technology lingo and the environment in which he operated.

During the interview, Thomas would often take long moments to consider his thoughts before speaking. There were a couple of points in the interview where he nodded his head back and forth, deep in thought for what felt like a minute to a minute and ½. During his administrative response and support discussion, I could see his forehead wrinkle and upside-down frown, which were sometimes irreconcilable with his words. This left me suspicious as to his assertive stance on administrative support. I did not feel comfortable probing him on this matter.

I chose the initial codes: technology, cybersecurity, mobile, fear, hackers, victims, and administrative support. As the study progressed, I added open codes such as cloud solutions, vulnerability, organizational response, attack, breach, fear, severe and two-factor authentication, terrorists, and password protection. I was surprised to see the cloud solution show up as a code. It does make sense since this is the future of IT organizations' data security. It is something that I am not comfortable with because it feels like, as security experts, we are passing the buck to some invisible firm. The respondent seemed satisfied with this solution and supported continued migration to the cloud for all services.

My initial codes made sense because they were common themes I would expect in the IT environment, having worked in IT for over 20 years. Technology was meant to describe discussion regarding networks, routers, computers, and other physical components. I quickly realized that the term was too broad. I noticed that Thomas refrained from going into the weeds in our discussions. Had he gone into deeper depth, he would have had to discuss security for each of those components., Nevertheless, at the time, I was not sure about such a granular level of security measures. As the conversation moved forward, I decided to do some open coding for other emerging themes.

Another start code that I chose was cybersecurity. This word was supposed to be the theme of any cyber defense implemented to prevent an attack or breach. This was an obvious code, and it emerged from the interview. Additionally, mobile was an initial code. I thought Thomas would discuss mobile applications for monitoring the servers and other computer systems that fell under his area of responsibility. He, however, mentioned his mobile phone a limited number of times, and it turned out he did not use it that much in the way that I thought he might have.

The third that I chose was fear. I anticipated that there would be high levels of anxiety or fear. It was expressed in the interview when Thomas discussed cyberattacks, breaches, and ransomware concerns. This assumption proved correct, as this was another consistent theme throughout the interview.

Two other codes that I started with were hackers and victims. I again assumed that there would be several stories regarding attempted breaches and many victims. Thomas surprised me when he stated that they had not had many security incidents. Although he did discuss one victim, there was no significant number of stories to support the use of the code, and there was no theme. He briefly mentioned the hackers as stories that occurred outside of his domain.

Administrative support was an initial code that I chose to show whether the administration was supporting or not supporting cybersecurity efforts. I was not confident about what the interview would reveal regarding this theme. However, administrative support was a powerful theme in Thomas's interview.

Open coding was performed for themes presented themselves as Thomas spoke during the interview. The first was cloud solutions. It turned out that Thomas was a proponent of cloud solutions, and the theme emerged quickly. The vulnerability was another theme that presented itself. A few times, Thomas mentioned the potential vulnerability of systems or the network, especially when discussing the network's physical security. I was surprised to hear this concern. I would have thought that the word vulnerability would have been reserved for user password and login inefficiencies or security protocol violations, but that was not the case. The administrative response was another open code. It emerged because Thomas continued to discuss how the administration would respond in different circumstances. It was clear that Thomas was convinced that the administration was very cyber aware and concerned.

Additionally, I coded for attack and breach. The two words are synonyms; however, a breach was a more specific instance of an attack. For example, in Thomas's story, a hacker may attack the organization's network, having limited success or no success. In comparison, a breach in the context of Thomas's interview would define an attack where sensitive data on the databases was successfully accessed by malicious actors. Therefore, the breach was an extreme case of an attack.

I also coded for serious. This was because there were times during the conversation when he would take on a more serious tone to discuss a topic. This was especially notable when he discussed breaches and considered fear. I also coded for two-factor authentication but then regretted it as he only mentioned it once, and there was no theme for this code. I should have just left it under the category of cybersecurity. I also coded for terrorists, but Thomas only mentioned it once, and there was no theme. I also regret coding for password protection as it was only said once or twice and could easily fall under cybersecurity.

Two dominant themes that emerged were "cybersecurity" and "attack." These two themes were expected because they are the primary concerns of a cybersecurity expert. Thomas was primarily concerned with attacks on the systems. Of course, cybersecurity in the context of the interview involves the actions in place by both applications and Thomas to prevent or blunt the effects of an attack by malicious actors.

In conclusion, Thomas is a cybersecurity professional who has a powerful desire to remain in the field and increase his level of responsibility by adding industry certifications. He displayed moderate anxiety levels on specific topics such as administration discussions; however, his overall mood was happy, as indicated by his body language. He often smiled, sat straight, and held my gaze when considering answers. I felt as if he judged whether he could trust me with what he wanted to say in those moments. Time ran over before I could get to questions about security modifications due to state and federal regulations. Future questions should delve into the issues of fear and administration response to cyber-attacks.